

# COIN Security

## draft-urien-coin-sec-01.txt

Pascal.Urien@Telecom-Paris.fr

# About COIN

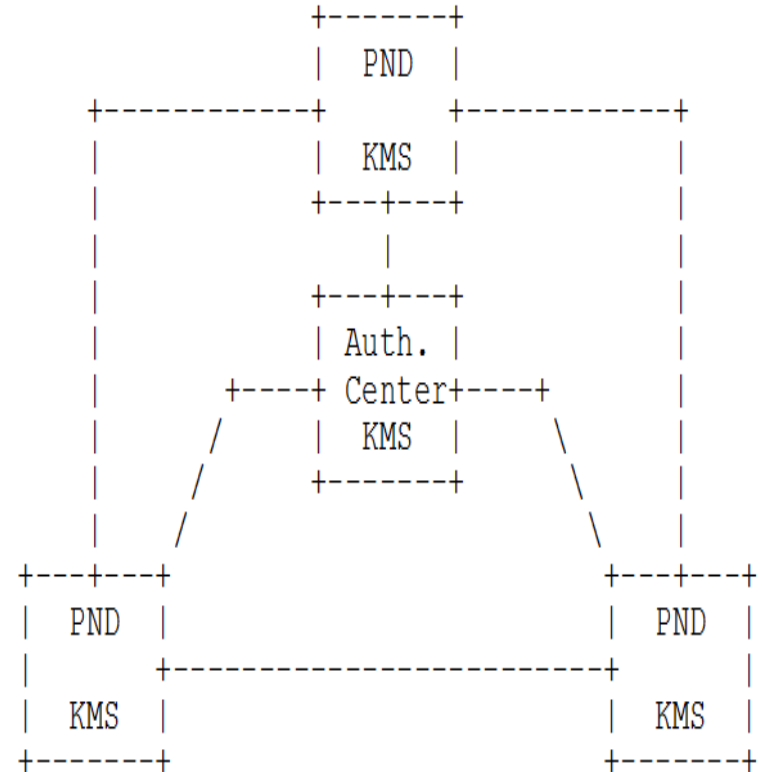
- Computing in the Network (COIN) is a concept that aims at deploying and using programs, based on computing resources hosted in Programmable Network Devices (PNDs).
  - Such infrastructures could be integrated in edge computing or 5G slicing.
- A program works with several PNDs exchanging data over secure communications.
- In that context there is a need for security
  - for intrinsic (infrastructure) COIN needs
  - for programs running in COIN systems

# Intrinsic COIN Security

- COIN should rely on fully encrypted communications, what implies authentication and keying mechanisms based on symmetric or asymmetric secrets.
- Should COIN include billing mechanism ?

# COIN Infrastructure Security

- PND should include Key Management System (KMS) in order to provide these security features.
- If COIN services rely on centralized architecture an Authentication Center (AC) should provide KMS functionalities.
- PND processors can also include a physical entity with isolated (for example Trusted Execution Environment, TEE) or tamper resistant computing resources (sometimes refers as integrated secure element iSE).

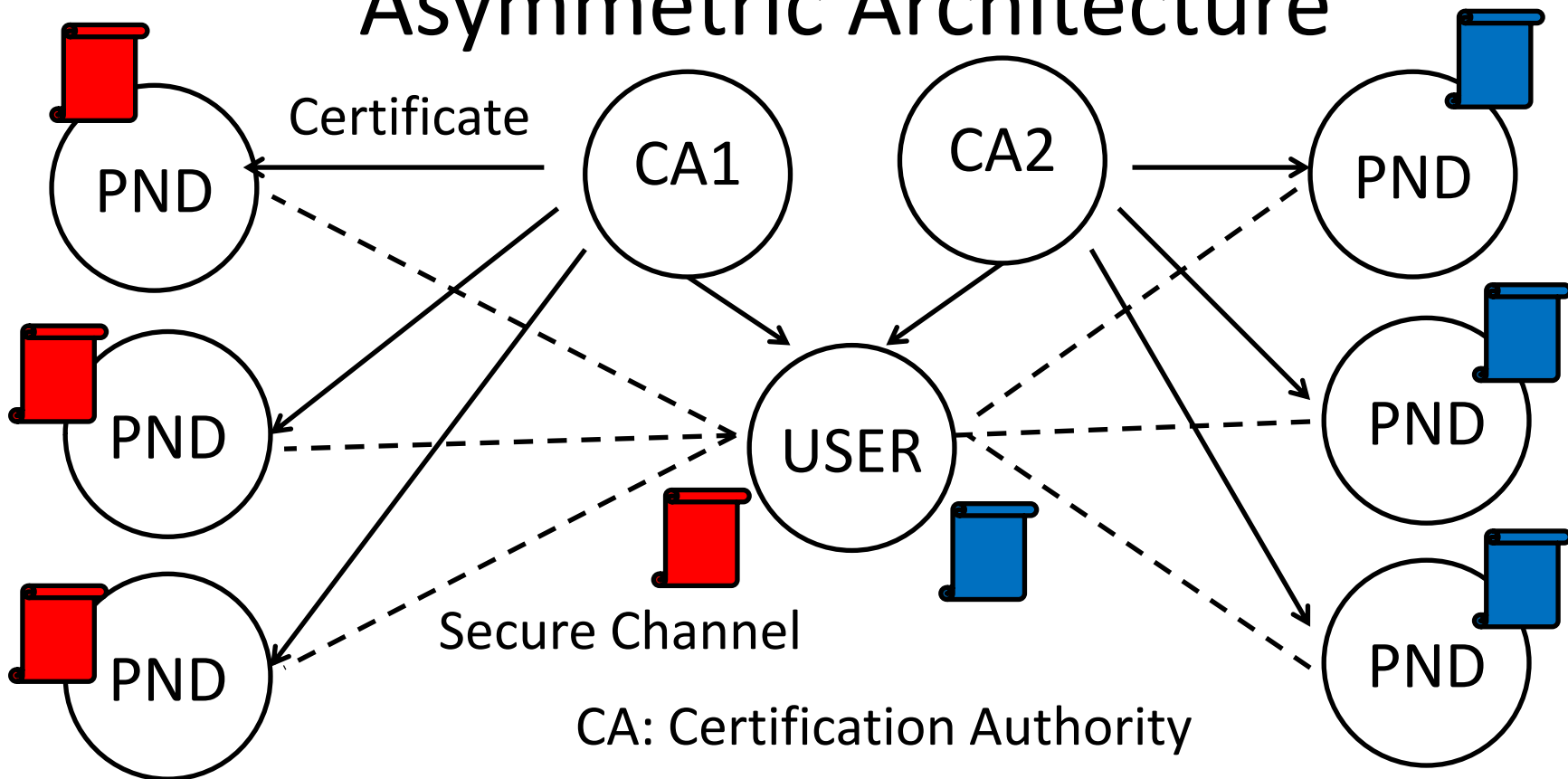




# Identity

- Identity is used to identify and authenticate PNDs.
- Identity knowledge should provide information about computing resources and trust level.
- An entirely distributed architecture could use asymmetric cryptographic and certificates to identify participating PNDs and associated computing resources.
- Single tenant architectures will likely use symmetric cryptographic algorithms and single authentication center. Secure data exchanges could occur in a way similar to cellular network communications.
- Multi tenant architectures should involve several authentication centers. Secure data exchanges could occur in a way similar to cellular network communications.

# Single / Multiple Tenant Distributed Asymmetric Architecture



# Single / Multiple Tenant Centralized Symmetric Architecture

